FORT LEONARD WOOD ACCESS INFO SHEET

The following items are required to set up your FLW student computer account.

1. This completed Form
2. DoD Information Assurance Awareness training certificate, less than 1 year old. You can take the training at https://ia.gordon.army.mil/dodiaa/default.asp
3. Signed Computer User Agreement. (Attached)
4. ID Card. If you do not know your PIN then you must go to the ID Card Section at BLDG 470 and have it reset.

Once all information is collected, this form filled out and the Computer User Agreement is signed, turn them into the student class leader or the course coordinator for further processing.

If you currently have an email address at any US Installation, you will need to be deleted from their system prior to obtaining a Fort Leonard Wood Account.

If you already have a Fort Leonard Wood email account, what unit is it with? _____

Please contact the IASO of that unit to be deleted from their mailgroup so a new mailgroup can be created for your student account. You will not lose any messages in your account.

Write Legibly!!!!

COMPONENT: RA ARNG USAR (Circle One) EPID (CAC #)_____

NAME OF CLASS: _____ **COURSE NUMBER:** _____

COURSE DATES: _____ **to** _____

UNIT PHONE: (573)596-0800 BLDG #: 1702E RANK/GRADE: _____

LAST NAME: _____**FIRST NAME:** _____ **MI:** ___

SUFFIX: _____ **AKO USER ID:** _____ **LAST 4 SSN:** _____

Name_____ **Course #** _____

ACCEPTABLE USE POLICY (AUP) July 14, 2008 - Rev 11

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in the Secret Internet Protocol Router Network (SIPRNET) and/or Non-secure Internet Protocol Router Network (NIPRNET) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. Access. You are accessing a U.S. Government (USG) information system (IS) (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only as set forth in DOD Directives 5500.7-R (Joint Ethics Regulation), IAW AR 25-2 (Information Assurance), Ft. Leonard Wood (FLW) Local Command Policy 41-08, UCMJ, and Army network policy and accreditation.

3. Revocability. Access to USG IS resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. SIPRNET is the primary classified IS for FLW Organizations. SIPRNET is a classified only system and approved to process SECRET collateral information as SECRET and with SECRET handling instructions. The classification boundary between SIPRNET and NIPRNET requires vigilance and attention by all users.

5. Unclassified information processing. NIPRNET is the primary unclassified IS for FLW Organizations. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2 and local automated information system security management policies.

6. Mandatory DoD acceptable use notification:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

a. At any time, the U.S. Government may inspect and seize data stored on this information system.

b. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

c. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

d. Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

e. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

f. All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

6. User Minimum-security rules and requirements. As a SIPRNET and/or NIPRNET system user, You consent to the following conditions:

a. Properly requesting access to any computer or automated IS on FLW. My approved access level will not be exceeded. If I have gained access to an area I should not, I will report this information to my Information Assurance Security Officer (IASO). I will not disseminate information to anyone without a verified need-to-know. It is my responsibility to properly mark and label all media and documentation appropriately.

b. Completing annual security awareness-training (e.g., Annual IA Awareness Training or Computer Security for Users) I will provide proof of completion to my IASO.

c. Securing my authentication credentials (UserID, password, CAC and CAC PIN) and email account. These are unique to me, and will not be shared. Nor will I log in and allow someone else to use my session. I will be held responsible for events that take place under my credentials. Any time I step away from my IS, I will lock the workstation, or log off. I will log off at the end of each day. It is imperative that my CAC not be left unattended.

d. Personally owned hardware (e.g., thumb drives, wireless access points) and software (e.g., free/shareware, P2P) are not allowed on Government networks.

e. Physical relocation or changes to configuration or network connectivity of IS equipment will be done by authorized personnel only. I will leave my Government IS connected to the network at all times. I will not attempt to interfere with IA patching and updating requirements. I will comply with security guidance issued by my SA/IASO.

f. Protecting the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from ANY removable storage media. I will ensure anti-virus definitions are updated regularly as a necessary security measure.

g. Government Computers (GC) are for official and authorized purposes only; as is official email, which is prohibited by AR 25-2 to be auto-forwarded to a non-official account. Unethical and illegal use of IS include but is not limited to: Spam/chain mail, profanity, sexual misconduct, gaming, extortion, racial or discriminatory epithets, file-sharing, personal use for financial gain, chatting/instant messaging (except as provided through AKO), pornography, etc.

h. Altering, changing, configuring, or using operating systems, programs (e.g., security/protective software and associated logs), or IS except as specifically authorized, is not allowed. All maintenance/modification will be performed by a certified System Administrator (SA) or DOIM technician only. I may not introduce executable code (e.g., .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code. I will immediately report any suspicious output, files, shortcuts, or system problems to the FLW Unit/Organization IASO or the DOIM Help Desk (3HELP/3.4357) and cease all activities on the system.

i. Mobile computing devices (MCDs) and removable media storage devices will be encrypted utilizing Data-at-Rest technology such as the Microsoft EFS or other Army authorized encrypting software (i.e., Mobile Armor).

j. Not participating in any use that could cause congestion, delay, degradation or disruption of service to any government IS or equipment is unacceptable (e.g., video, sound or other large files, and continuous data streams).

k. Not attempting to strain, test, circumvent, or bypass network or IS security mechanisms, or perform network or keystroke monitoring. I will not run software that monitors network traffic or any hacker-related software on a government computer, government IS, or network.

l. I understand that I may use a USG IS for limited personal communications by e-mail and brief internet use provided that my usage is in compliance with written unit policy established by my Commander/Director, and that such use does not cause an adverse impact on the network.

m. I understand that a violation of this AUP or AR 25-2 security measures will result in the loss of my privilege. I further understand that I will receive a written counseling statement from my first supervisor. In order to lift this restriction, a memorandum from my Commander/Director (or designated representative) will be required. This request will be routed via the IASO to the installation IAM.

7. IMPORTANT: This electronic AUP must be digitally signed within 24 hours of receipt or the network account will be suspended. A digitally signed email is the preferred method. However, in the event that it is not possible, print and sign this form, and provide the original to the Unit/Organization IASO. The Unit/Organization IASO will update the UserID Management System (UMS) during the 24 hour grace period, and will maintain it for Unit retention.

8. By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems you agree to the above stipulations.

9. Acknowledgement. I have read, understood, and agree to the terms and conditions in this AUP.

DOTLD/DOI		(573) 596-0800
Directorate/Division/Branch	Date	Area Code and Phone Number

Last Name, First, MI (Print)	Rank/Grade and Last Four of SSN Signature